09-29-00

A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
UTILITY PATENT APPLICATION TRANSMITTAL
UNDER 37 CFR 1.53(b)

Address to:	*Attorney Docket No.*	**ARC9–2000-0091-US1**
Assistant Commissioner for Patents	*Inventor(s)*	**ZIMMERMAN, Thomas Guthrie**
Box Patent Application	*Express Mail Label No.*	**EL537037798US**
Washington, DC 20231	*Total Pages*	**49 (Not including references)**

Title of Application:

"SYSTEM AND METHOD FOR PROVIDING TIME-LIMITED ACCESS TO PEOPLE, OBJECTS AND SERVICES"

Transmitted with the patent application are the following:

1	Page(s)	Transmittal form (and one copy)
34	Page(s)	Specification, claims, abstract
5	Page(s)	Formal Drawings
2	Page(s)	Declaration and Power of Attorney
1	Page(s)	Recordation of Assignment
1	Page(s)	Assignment of the Invention to International Business Machines Corporation
1	Page(s)	Form 1449A
12	References	Cited in Form 1449A
1	Page(s)	Return Receipt Postcard (MPEP 503)
1	Page(s)	Check No. 1054 to cover the filing fee

This application is a: __ ***Continuation*** __ ***Divisional*** __ ***Continuation-in-Part of prior application Serial No.*** ______________.

Fee Calculation

	Claims		Extra	Rate	Fees
Basic Fee					$ 690.00
Total Claims	39	-20 =	19	× $18.00	$342.00
Independent Claims	3	- 3 =	0	× $78.00	$ 0.00
Multiple Dependent Claim				+	
				Assignm	$ 40.00
				TOTAL	$1072.00

The Commissioner is hereby authorized to credit overpayments or charge fees required under 37 CFR 1.16 or 1.17 to Deposit Account No. **50-0219**. Duplicate sheet attached.

EXPRESS MAIL CERTIFICATE

I hereby certify that the above paper/fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, DC 20231

Date of Deposit: 09/28/2000

Person mailing paper/fee: Samuel A. Kassatly

Signature________________

Respectfully submitted,
ZIMMERMAN, Thomas

Samuel A. Kassatly
Reg. No. 32,247
Attorney for Applicants
Telephone: 408-323-5111
Samuel A. Kassatly Law Office
6819 Trinidad Drive
San Jose, CA 95120-2056

SYSTEM AND METHOD FOR PROVIDING TIME-LIMITED ACCESS TO PEOPLE, OBJECTS AND SERVICES

CROSS REFERENCE TO RELATED APPLICATION

The present application is related to co-pending U.S. patent application, Serial No. 09/234,229, titled “System and Method for Optimizing Personal Area Network Electrostatic Communication,” which was filed on January 20, 1999, which is assigned to the same assignee as the present invention, and which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

The present invention generally relates to the field of electronic communication systems. More specifically, the invention relates to the use of personal encoded identification media for providing time-limited access to people, objects, information, services, and other resources. The invention has particular applicability to credit cards, dining cards; telephone calling cards; health cards; driver's licenses; video store cards; car access cards; computer access cards; building access cards, identification tag; key fob and like ID badges and tokens.

BACKGROUND OF THE INVENTION

The use of electromagnetic fields as a communication medium is ubiquitous in today's society. Both communication over physical media, such as wires, and wireless communication, such as broadcast radio, television and satellite, infrared, and ultrasound, are widespread and commonplace. Such communication may be made over long distances, or over much shorter distances, such as closed-circuit television or a client human being using a terminal to communicate with a local server. Other media may be used for wireless communication, including acoustic such as ultrasonic, sonic, and subsonic, electric field and magnetic field.

In some situations, a user is physically present at a terminal or communication system, for the duration of a transaction. The terminal is available to all interested users, and a user having need of the service provided by the terminal seeks it out and uses it to make the transaction. Examples of such terminals are public pay telephones and Automatic Teller Machines (ATM).

Many transactions involve the use of a portable instrumentality or an input device such as a keypad, for verifying the identity of the user in order to authorize the transaction, make a charge for the service, etc. Often, this portable instrumentality takes the form of a card or badge bearing a magnetically encoded stripe, which is readable by the terminal. For instance, a user seeking cash from an ATM stands before the ATM, inserts his/her card, and keys in a Personal Identification Number (PIN), followed by menu-prompted transaction instructions. Authorization of the transaction is based on a verification of the user's identity based on a combination of (i) the user's possession of the authorizing card, and (ii) the user's knowledge of the PIN.

However, this form of communication could expose the user to physical hazards, and the card to theft and unauthorized access. U.S. Patent No. 5,796,827 to Coppersmith et al, which is incorporated herein by reference, addressed this problem by providing an apparatus and method for utilizing the human body as a communication medium to transmit information related to the user, to protect the user's privacy and the confidentiality of the information against unauthorized access. The patented communication system produces small currents in the human body, externally induced by electrostatic field coupling, which provides for wireless identification and authentication among proximate devices. The system encrypts data and provides for easy and rapid receipt and authentication of the encrypted data, with sufficient capacity to handle millions of unique transmitter codes.

U.S. Patent No. 5,657,388 to Weiss describes an attempt at improving the secure access to electronic information by utilizing a token that may contain a public ID, to provide secure access by authorized users to a selected resource. The token stores a secret user code in machine readable form, which code is read by a token processor. The token processor receives a time-varying value and an algorithm, both of which may be stored or generated at either the token or the token processor, and a secret personal identification code which may be inputted at the token or the token processor. The secret user code, time-varying value, and secret personal identification code are then algorithmically combined by the algorithm to generate a one-time nonpredictable code which is transmitted to a host processor. The host processor utilizes the received one-time nonpredictable code to determine if the user is authorized access to the resource and grants access to the resource if the user is determined to be authorized.

However, the systems described in U.S. Patent No. 5,657,388 and other similar publications still rely on the transmission of a public key or other public ID for proper authentication. The public ID which typically includes a static code value is also subject to surreptitious detection, and can be used to associate a particular user or object with a specific transmission, compromising the user's or object's privacy.

While conventional devices have provided significantly enhanced security for data processing systems, databases and other information resources there still remains an unsatisfied need for a further improved system that eliminates the need for public keys or IDs, thus further minimizing invasion of privacy, security risk and exposure.

As an example, though identification badges that wirelessly transmit an ID code can be used to locate someone in a building, such as to find doctors in a hospital, maintenance people in a factory, or key personnel in an office, individual privacy might be compromised in that the badge users can be tracked all the time without their control or consent. It would therefore be desirable to have a system that limits access to tracking information, such as allowing a badge user to be tracked for limited time periods that are determined by this particular user.

SUMMARY OF THE INVENTION

One feature of the present invention is to provide a limited tracking system and associated method that enable the use of personal encoded identification media to limit access to tracking information.

A more specific feature of the limited tracking system is to provide concurrent time-limited access to a large number of people, objects, information, services, and other resources, which are herein collectively referred to as “resources”. The limited tracking system has particular applicability to credit cards, dining cards, telephone calling cards, health cards, driver's licenses, video store cards, car access cards, building access cards, computer access cards, and like identification badges or cards.

For example, the limited tracking system could allow persons to be tracked only during business hours but not during lunch or break times. This will allow privacy of movement during the employee's personal time. Alternatively, the limited tracking system could be automatically tied to events in a person’s or group’s calendar, to allow tracking during important meetings or phone calls, so that an assistant might try to locate individuals during these important events. The limited tracking system can be included in laptops, desktops or processors, to track assets in buildings.

Another feature of the limited tracking system is to distribute tracking access to multiple sources and limit the vulnerability of a user's or object's privacy if one or more of the sources are compromised.

The foregoing and other objects and features of the present invention are realized by a limited tracking system that includes a transmitter module incorporated in an ID badge, card, or label, and a receiver module incorporated in a secure server. The transmitter module contains a microprocessor and a watch crystal that keeps track of time. The microprocessor encrypts time with a private key, and transmits the encrypted time once every ten seconds. The transmission can be any wireless means, including infrared, radio frequency, electric field, magnetic field, ultrasonics, and so forth. The limited tracking system is capable of individually tracking a large number of receivers that are distributed about one or multiple tracking environments or ranges.

The secure server stores the private keys of all the users (or receivers). The user of the badge can give a third party, or multiple parties, referred to herein as finder, access to the user for specified time periods. As an example, if the user wishes to give the finder tracking access for specific time periods, the user instructs the server to deliver a list of encrypted codes with the user's private key for these time periods. This list can be transmitted or otherwise provided to the finder for storage on the finder's own server. When the finder detects a transmission from the user's badge, the finder's server looks up the current value of the user's badge from the list and compares it to the encrypted code it received from the badge. If a match exists, the finder would have identified and located the user.

BRIEF DESCRIPTION OF THE DRAWINGS

The various features of the present invention and the manner of attaining them will be described in greater detail with reference to the following description, claims, and drawings, wherein reference numerals are reused, where appropriate, to indicate a correspondence between the referenced items, and wherein:

FIG. 1 is a schematic illustration of an exemplary operating environment in which a limited tracking system of the present invention may be used, showing a plurality of badges in communication with a base receiver, a processor, and a server, for access authentication;

FIG. 2 is a high level functional block diagram of an exemplary badge Bn shown in communication with a receiver module that forms part of the base receiver of FIG. 1;

FIG. 3 is a high level functional block diagram of an exemplary badge Bn;

FIG. 4 is a flow chart illustrating an exemplary encryption process implemented by the badge of FIG. 3 according to the present invention, for transmitting an encrypted code specific to each badge;

FIG. 5 is a flow chart illustrating an exemplary access authentication process implemented by either the processor of FIG. 2, or the local processor, the remote processor and/or the server of FIG. 3, for authenticating the encrypted code transmitted by the badge according to the process of FIG. 4; and

FIG. 6 is a high level functional block diagram of an exemplary badge Bn shown in communication with a third party receiver and the receiver module of limited tracking system of FIGS. 2 and 3.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 depicts a plurality of badges, cards, persons B1-Bn, hereinafter referred to collectively as either "user(s)" or badge(s)", each provided with a component of a limited tracking system 10 of the present invention, and shown in communication with a base receiver 20, a processor 30, and a server 40, for time-limited access authentication according to the present invention. It will be understood that numerous other environments may also employ the limited tracking system 10. Such other environments may include, for example, public telephones that accept calling card calls, gas pumps at service stations, photocopy machines, postal meters, and entry through building or automobile doors. Also, the limited tracking system 10 may be used in connection with the computer or processor 30 as a log-in mechanism. In addition, while only one base receiver 20, processor 30, and server 40 are shown for illustration purpose only, it should be clear that additional base receivers 20, processors 30, and/or servers 40 may be used for a decentralized limited tracking system 10.

In operation, each badge B1-Bn generates a temporal sequence of values, encrypts the temporal sequence with a private key associated with the individual badge B1-Bn, and transmits at a predetermined transmission cycle an encrypted code element, for example one every ten seconds In a preferred embodiment a time keeper provides the temporal sequence of values. The resulting encrypted code element, appears to the observer as a random number. As an alternative, the encryption and transmission can be initiated by mechanical means, such as a electrical switch on the badge, or a motion detector. For example, each time the switch is pressed, an encrypted code element is calculated and transmitted. As one (or more) badge B1-Bn enters a communication zone 50, denoted by a circle in dashed line, associated with the base receiver 20, the encrypted code for that badge is transmitted to the base receiver 20 over a communication link 60. The transmission can be any wireless means, including infrared, radio frequency, electric field, magnetic field, ultrasonic, and so forth. The transmission can also be by contact, such as a smart card, or by physical contact as described, for example, in U.S. Patent No. 5,796,827 to Coppersmith et al, which is incorporated herein by reference. Alternatively, at least a part of the transmission link 60 is wireless. The limited tracking system 10 is capable of individually tracking a large number of badges B1-Bn that are distributed about a tracking environment or communication zone 50.

In accordance with the present invention, the communication between the badges B1-Bn and the base receiver 20 is encrypted to establish authentication and security. A preferred technique of encryption is described in detail below. Also, if the user carries multiple badges (i.e., transmitters), such as instrumentalities embedded in cards, a watch, or shoes, these badges may be detected separately for authentication.

In accordance with the present invention, and as illustrated in FIG. 1, a badge Bn transmitter and a base receiver 20 work in combination to provide unidirectional communication. For bidirectional communication, the badge Bn can be provided with a receiver, and the processor 30 can be provided with a receiver. For a unidirectional badge Bn, time is the challenge, and time encrypted by the private key is the response. For a bi-directional communication, the base receiver 20 includes a transmitter which transmits a challenge to the badge Bn. The badge Bn encrypts the challenge by the private key and transmits the response to the base receiver 20.

FIGS. 2 and 3 are block diagrams of two preferred embodiments of the limited tracking system 10 of the present invention. Unidirectional communication takes place between a badge Bn, and a receiver module 100 that forms part of the base receiver 20. The limited tracking system 10 supports a scenario in which the badge Bn continuously, or at regular intervals such as every ten seconds, transmits an encrypted code as described herein.

The badge Bn generally includes an encryptor 111 that generates an encrypted code based on a private key (or a user ID) dedicated to the badge Bn and a time representation. The resultant encrypted code can optionally be modulated using a modulator, known to the art of digital communication, such as amplitude modulation, frequency modulation, and spread spectrum (not shown) and transmitted to the receiver module 100 by means of a transmitter unit 120.

The receiver module 100 is coupled to the communication link 60 for receiving the encrypted code. To this end, the receiver module 100 includes a receiver unit 130 that receives the encrypted code and optionally demodulates it. The received encrypted code is then passed to the server 40. The server 40 includes an authenticator 140 that authenticates the signal as described in detail below, and provides the information to an application such as a program for confirming the presence of the badge Bn.

The server 40 uniquely identifies the user or the badge Bn, rejecting attempts at impersonation. A sample application would be a unique ID card for a population of several hundred (i.e., 500) employees working in a building, each of whom using a badge for access to the building and/or other services.

With reference to FIG. 3, each user or badge Bn has a unique private key or ID Xn (also reference by the numeral 200), represented by a bit-string, typically of length 56 or 128 bits. At ten-second intervals as measured by a clock crystal 210, the badge

Bn transmits a signal f(X,t) (represented as a bit-string), where f() is an encryption function which is computed by the encryptor 111, Xn is the user's unique private key, and t is the time (in seconds) measured, for example, from an initial synchronized starting point of the badge Bn.

According to another embodiment, a network of base receivers 20 can be dispersed in a geographic area to track the whereabouts of the badges B1-Bn.

When the badge Bn enters the communication zone 50, the limited tracking system 10 attempts to discover the identity of the Bn. The receiver unit 130 (FIG. 2) receives the encrypted code, and sends the encrypted code to the server 40. In turn, the server 40 sends the encrypted code to the authenticator 140. The authenticator 140 creates an authentication table composed of pre-calculated encryptions for every expected badge Bn for the current time. Upon receiving an encrypted code, the authenticator 140 attempts to find the encrypted code in the authentication table. In a preferred embodiment, an identification number, private key Xn, and offset time value (to be described later) of every badge Bn is stored in a database 260. The authenticator 140 checks whether or not the decrypted signal matches authenticating codes that are stored in the database 260 of the server 40, for this particular badge Bn, during a specified time window, that generally corresponds to the badge's entry into the communication zone 50. If the encrypted code is in the authentication table, the authenticator 140 sends the badge Bn identification number back to the server 40, else it sends a "not found" message to the server 40.

It should be noted that the signal or code transmitted by the badge Bn, includes the badge's time encrypted by the private key Xn, but does not include a public ID as was taught by conventional tracking systems. As a result, the encrypted code transmitted by the badge Bn can only be decrypted by a private, non-public key which is available only to the server 40 and to the badge Bn.

Time increments, and the encryption of time, produce a random sequence of numbers that are transmitted. Because the badge Bn sends out what appears to be random numbers, an eavesdropper would see gibberish (random numbers) which would not reveal any information about the carrier of the badge Bn. It is only when these numbers are sent to the authenticator 140 that they are linked with a service, such as an ATM, drivers license, calling card, etc. Detecting the transmission of the badge Bn does not reveal the identity of the user, nor can a relation be made between a current transmission and previous ones, without knowledge of the private key. In this way, anonymousity of the user is maintained.

Referring to FIG. 3, the badge Bn contains a clock 210, private key Xn 200, encryptor 111, and wireless transmitter 120. The clock 210 provides the current time, and includes a time reference, preferably a quartz crystal oscillating at 31.768 kHz. In a preferred embodiment, the current time is the elapsed time in seconds since the badge Bn was manufactured. The encryptor 111 in the badge Bn uses an encryption that can be, for example, the well-known Data Encryption Standard (DES). The encryptor 111 periodically encrypts time (t) with the private key Xn 200, and transmits the result using the transmitter 120.

Referring to the flow chart of FIG. 4, it illustrates an exemplary encryption and transmission method 400 implemented by the badge Bn according to the present invention. The method 400 starts at step 410 and inquires at decision step 420 if a predetermined period of time (i.e. the predetermined transmission cycle), such as 10 seconds, has elapsed since the last transmission by the badge Bn. If the elapsed time still has not exceeded the predetermined period, the method 400 returns to decision step 420 and repeats the inquiry until the elapsed time exceeds the set time period. At which stage, the method 400 proceeds to step 430 where it resets the elapsed time interval.

The method 400 then proceeds to step 440 where the DES encryptor 111 of FIG. 3 encrypts the time for the badge Bn by the user's private key Xn, as can be represented by the following expression:

$$f(Xn,t) = (T_{Bn})_{Kn},$$

where (T_{Bn}) represents the time for the badge, Kn represents the private Key for the badge Bn, and where n varies in the above example from 1 badge to 500 badges.

At step 450 the transmitter unit 120 transmits the encrypted code $(T_{Bn})_{Kn}$ to the receiver module 100 and the server 40, and then returns to decision step 420 for repeating steps 430-450. As it will be described in connection with FIG. 5, the receiver module 100 and the server 40 receive and authenticate the encrypted code $(T_{Bn})_{Kn}$. The server 40 then looks up the private key Xn that has generated the encrypted code $(T_{Bn})_{Kn}$, and from this private key Xn, the server 40 identifies the badge Bn. In one implementation, the badge Bn requires about 96 bits of RAM to implement the DES encryption, another 64 bits for the time tn, and a few thousand bits of ROM for the DES encryption. Faster implementations of DES would require for example approximately 32K bits of ROM.

Referring now to FIG. 5, it illustrates an exemplary access authentication method 500 which is implemented by either the processor 30 of FIG. 2 for authenticating the encrypted code $(T_{Bn})_{Kn}$ transmitted by the badge Bn. The authentication method 500 starts at step 510 and inquires at decision step 420 if a predetermined period of time, such as 1 second, has elapsed since the last reception cycle. In a preferred embodiment the temporal resolution of the authentication table, determined by the period at step 520 of FIG. 5 should be equal to, or greater than the predetermined transmission cycle 420 of FIG. 4, so the authenticator 140 has equal or greater temporal resolution than the badges Bn.

If the authentication method 500 determines at the decision step 520 that the elapsed time still has not exceeded the predetermined period, the method 500 determines at decision step 525 if a valid badge packet has been received. To this end, the packet transmitted by the badge Bn typically includes three fields: a preamble field, a payload field, and a checksum field.

The preamble contains data bits indicating that the packet is originating from a valid badge, or otherwise a badge associated with the limited tracking system 10. This precautionary measure allows the limited tracking system 10 to filter out transmissions, noise, or otherwise irrelevant signals, and to process only related signals. The payload field contains the encrypted code $(T_{Bn})_{Kn}$ described earlier, which will eventually be processed by the receiver module 100 for badge authentication. The checksum field provides means for checking the integrity of the transmission.

If the authentication method 500 determines at the decision step 525 that the received packet is not a valid badge packet, by for example analyzing the preamble field content or the checksum is not correct, the method 500 ignores the packet and returns to the decision step 520, where it repeats the inquiry until the elapsed time exceeds the set time period.

At this stage, the method 500 proceeds to step 530 where the elapsed time count is reset. The method 500 then proceeds to step 540 and encrypts the sum of the current time badge Bn time (T_{Bn}) and offset time value (T_{on}) with respect to the private key Xn for all the valid the badges B1-Bn, as represented by the following expression:

$$En = (T_{Bn} + T_{on})Kn,$$

where T_{on} is the offset time or time drift for each badge Bn which will be explained in the next paragraphs, En is the encrypted result for badge n, T_{Bn} is the time for badge n, Kn is the key for badge n, and T_{on} is the time drift for badge n. Initially, T_{on} is set to zero the first time it is detected, and is modified based on successive authentications of the badge Bn.

Since the badge Bn does not transmit the time, the current time badge Bn time (T_{Bn}) is calculated by the authenticator 140 by the following expression;

$$(T_{Bn})=T_{system}-T_{badge\ n\ creation}$$

where T_{system} is the current server 40 system time in seconds and $T_{badge\ n\ creation}$ is the time the badge Bn was created, referenced to the same time standard as T_{system}. The $T_{badge\ n\ creation}$ for each badge Bn is stored on the database 260.

One problem addressed by the present invention is time drift that develops between the badge Bn and the authenticator 140. There are generally two main causes for the time drift: (a) systematic, the time reference of a particular badge Bn is faster or slower than the authenticator 140; and (b) random, the time reference of a particular badge Bn usually varies due to temperature or other environmental changes.

The first cause is predictable, and in a preferred embodiment the authenticator 140 calculates the frequency of each badge B1-Bn from successive authentications. Time drifts due to temperature changes are usually minimal, since the badge Bn is typically kept with a person at room temperature. The stability of practical time references are demonstrated by the time keeping ability of inexpensive digital watches that can maintain time to within a few minutes per year.

Another feature of the present invention is the establishment of a window of tolerance (also referred to as a clock synchronization window, drift window, or temporal tolerance window) for the encrypted result, En, in order to allow authentication in the presence of time drift. Since the clocks 210 (FIG. 3) of the badges B1-Bn and the clock at the server 40 cannot be expected to remain in perfect synchrony, the server 40 allows a clock synchronization window within which authentication would proceed.

According to one embodiment, the server 40 allows authentication within a "drift window" centered around the time T_{Bn} of the badge Bn, as shown by the following expressions:

$$En1 = (T_{Bn} + T_{on})_{Kn},$$

$$En2 = (T_{Bn} + T_{on} - Epsilon)_{Kn}, \text{ and}$$

$$En3 = (T_{Bn} + T_{on} + Epsilon)_{Kn},$$

where Epsilon is the transmission cycle.

In this embodiment, En1 is the encrypted results when the badge Bn is in synchrony with the server 40 (to within +/- one half of a transmission cycle). En2 is the encrypted results when the badge Bn lags the server 40 by one transmission cycle (+/- on half a transmission cycle). En3 is the encrypted results when the badge Bn leads the server 40 by one transmission cycle (+/- on half a transmission cycle). In this example, the drift window is 2 transmission cycles, that is the badge Bn can lead or lag the server 40 by one transmission cycle. In this example, and in the preferred embodiment, the temporal resolution (increment size) of the temporal sequence of values generated in the badge Bn is equal to the transmission cycle.

As stated earlier, the intially T_{on} is set to zero on the first read of the Badge Bn by the server 40, and is modified based on successive authentications of the badge Bn. If the badge Bn authenticates with E1, T_{on} remains the same. If the badge Bn authenticates with E2, T_{on} is decremented ($T_{on} = T_{on} -1$). If the badge Bn authenticates with E3, T_{on} is incremented ($T_{on} = T_{on} +1$). By this method, the authenticator 140 tracks drift in the badge Bn clock 210, preventing the drift from accumulating and preventing authentication. A more sophisticated method of correcting for drift is to observe the drift over time, calculate the slope of drift, store the slope for each badge Bn, and calculate T_{on} based on the slope of drift. This would compensate for systematic drift in the badge, i.e. the time reference of a particular badge Bn is faster or slower than the authenticator 140;

A typical exemplary value for the synchronization window can be approximately 20 seconds. This function is implemented by a synchronizer 285 at the server 40 (FIG 2).

Upon completion of the encryption of step 540, the authentication method 500 proceeds to decision step 525 and checks the validity of the received packet as explained earlier. If at step 525 it is determined that the received packet has originated from a valid badge Bn, it proceeds to step 550 where it looks up the received encrypted code $(T_{Bn})_{Kn}$ in the server database 260.

The server 40 then inquires at step 560 whether the encrypted code $(T_{Bn})_{Kn}$ is found in the database 260. If the encrypted code $(T_{Bn})_{Kn}$ is not found, the server 40 generates an alarm, whether visual or audible, advising the badge user of the procedure to follow to have the situation corrected. For example, the server 40 can advise the badge user to proceed to the security office to have the badge clock 210 resynchronized, by changing the badge's Ton entry in the database 260, or to provide permission to the service or access requested.

If, on the other hand, the encrypted code $(T_{Bn})_{Kn}$ is located in the database 260, the server 40 authenticates and identifies the badge Bn at step 580. Once the badge Bn is authenticated, the server 40 can execute an application at step 590, or alternatively, it can instruct the local processor 240 (FIG. 3) to execute the application. Exemplary applications include: allowing access to the building, logging on to a network, gaining access to a car, or dangerous piece of equipment like a medical machine that administers radiation, hydraulic pressing for stamping car doors, medical cabinets for dispensing narcotics, registers for dispensing cash, guns for shooting bullets, and so forth.

FIG. 6 describes a specific implementation of the limited tracking system 10. Either the processor 30 (FIG. 1) or the secure server 40 stores the private keys Kn of all the badges B1-Bn. The private keys Kn are not available to the third party as represented by block 252.

The user of the badge, e.g. badge Bn, can give the third party, also referred to herein as finder, access to the user's encrypted codes for specified time periods. To this end, the badge (Bn) user, using the processor 30 (FIG. 1) instructs the server 40 to deliver a list of encrypted codes, i.e., a list of the times encrypted with the user's private key, for specific time periods, to the third party's local processor 275.

The code list can be transmitted or otherwise provided to the finder, i.e., local processor 275 for storage on the local processor 275 for local autonomous authentication, or to the finder's own server 340 and database 360 for networked authentication. When the third party receiver 252 detects a transmission from the user's badge Bn, the third party receiver 252 sends the encrypted code to the local processor 275. If authentication is to take place locally, local processor 275 compares the encrypted code it received from the badge Bn to the code list stored in its internal memory (for example hard drive) indexed by the current time. The local processor 275 can keep time using an internal clock, or externally receive accurate time, for example from a trusted site on the internet. If a match exists, the third party local processor 275 confirms the detection of the user's (or badge Bn) location, for example giving the user access to the resources of local processor 252, including data and applications on the local hard drive.

In the example of networked authentication, the local processor 275 receives the encrypted code from the third party receiver 252 and sends it to the server 340. The server compares the encrypted code to the code list indexed by time. If a match exists, the server 340 sends a message confirming the detection of the badge Bn to the local processor 275. If no match exists, the server 340 sends a denying message to the server 340, that for example will prevent access to local processor 275 resources.

A more specific example of the use of the limited tracking system 10 of FIG. 6 is as follows: A user provides the local processor 275 with a list of encrypted codes that reflects the time periods during which tracking would be allowed, for example, from 12:00 PM to 1:30 PM weekdays. At 12:00:00 PM on Tuesday, the user's badge Bn transmits the code 3948573, while within the communication zone 50, and at 12:00:10 PM it transmits the code 93874832. The badge Bn continues to transmit updated encrypted codes periodically. The code list provided to the local processor 275 contains only valid entries or codes (i.e., 3948573, 93874832, etc.) for the time periods the user has specified, to grant selective and limited access, at these particular times, and not complete access independent of time.

It is to be understood that the specific embodiments that have been described herein are merely illustrative of certain applications of the principle of the present invention. Numerous modifications may be made without departing from the spirit and scope of the present invention.

What is claimed is:

1. A tracking system for use with an identification medium to provide time-limit access to a resource, comprising:

a transmitter module secured to the identification medium;

a receiver module in selective communication with the transmitter module;

the transmitter module including an encryptor and a time generator that generates a temporal sequence of values (T_{Bn}), wherein the encryptor encrypts the temporal sequence of values (T_{Bn}) with a private key K_n which is unique to the identification medium to generate a code list composed of encrypted code elements $(T_{Bn})K_n$, and wherein the transmitter module transmits one or more encrypted code elements $(T_{Bn})K_n$ to the receiver module; and

a server, connected to the receiver module, for storing the private key of the identification medium, and including an authenticator that authenticates one or more of the encrypted code elements of the code list.

2. The tracking system according to claim 1, for use with a plurality of identification media, each identification medium including a transmitter module and a unique private key for transmitting at least one or more of the encrypted code elements $(T_{Bn})K_n$ to the receiver module for authentication.

3. The tracking system according to claim 2, wherein the server stores private keys of the plurality of identification media.

4. The tracking system according to claim 3, wherein the receiver module provides unidirectional communication with at least one of the plurality of identification media.

5. The tracking system according to claim 3, wherein upon authenticating the identification medium, the authenticator provides authentication information to an application for initiating the application.

6. The tracking system according to claim 3, wherein the private key is represented by a bit-string having a length of at least 48 bits.

7. The tracking system according to claim 5, wherein the transmitter module transmits the encrypted code elements at a predetermined transmission cycle.

8. The tracking system according to claim 3, wherein the temporal sequence of values is measured from an initial synchronized starting point of each identification medium.

9. The tracking system according to claim 1, wherein the temporal sequence of values is incremented in equal time increments.

10. The tracking system according to claim 7, wherein the authenticator creates an authentication table composed of precalculated encrypted code elements for every identification medium, and further attempts to match the encrypted code elements transmitted by the transmitter module to the precalculated encrypted code elements in the authentication table.

11. The tracking system according to claim 10, wherein the server encrypts the temporal sequence of values (T_{Bn}) and an offset time value (T_{on}) for each identification medium with a corresponding unique private key K_n to generate a list of authentication codes, En, as represented by the following expression:

$$En = (T_{Bn} + T_{on})Kn.$$

12. The tracking system according to claim 11, wherein the temporal resolution of the authentication table exceeds the transmission cycle of the transmitter module.

13. The tracking system according to claim 12, wherein the temporal resolution of the authentication table is approximately 1 second; and

wherein the transmission cycle is approximately 10 seconds.

14. The tracking system according to claim 11, wherein the transmitter module transmits at least one encrypted code element to the receiver module as a packet; and

wherein the packet includes three fields: a preamble field, a payload field, and a checksum field.

15. The tracking system according to claim 14, wherein the preamble field contains data bits indicating that the packet is originating from a valid identification medium;

the payload field contains an encrypted code element $(T_{Bn})K_n$; and

wherein the checksum field allows for checking transmission integrity.

16. The tracking system according to claim 11, wherein the temporal sequence of values (T_{Bn}) is represented by the following expression;

$$(T_{Bn})=T_{system}-T_{n\ creation},$$

where T_{system} represents current time for the server, and $T_{n\ creation}$ represents a creation time of the identification medium referenced to a same time standard as T_{system};

and wherein the server stores $T_{n\ creation}$ for each identification medium.

17. The tracking system according to claim 16, wherein the server establishes a clock synchronization window for the list of authentication codes, En, to account for

time drift between the current time of the identification medium and a current time of the server.

18. The tracking system according to claim 17, wherein the clock synchronization window is centered around the current time (T_{Bn}) of the identification medium, as shown by the following expressions:

$$En1 = (T_{Bn} + T_{on})_{Kn},$$

$$En2 = (T_{Bn} + T_{on} - \text{Epsilon})_{Kn}, \text{ and}$$

$$En3 = (T_{Bn} + T_{on} + \text{Epsilon})_{Kn},$$

wherein En1 is the authentication code when the identification medium is in general synchrony with the server;

wherein En2 is the authentication code when the identification medium lags the server; and

wherein En3 is the authentication code when the identification medium leads the server;

wherein Epilson is the resolution of the temporal sequence of values (T_{Bn})

19. The tracking system according to claim 1, wherein the transmitter module is incorporated in any one or more of: an identification badge, a card, or a label.

20. The tracking system according to claim 19, wherein the identification medium includes any one or more of: a credit card, a dining card; a telephone calling card; a health card; a driver's license; a video store card; a car access card; a computer access card; or a building access card; an identification tag, a key fob.

21. A tracking method for use with a plurality of identification media to selectively provide time-limit access to a resource, comprising:

encrypting the temporal sequence of values (T_{Bn}) of the identification media with private keys K_n that are unique to each identification medium, to generate a transmission comprised of encrypted code elements $(T_{Bn})K_n$;

securely storing the private keys of the plurality of identification media; and

authenticating the transmitted encrypted code elements $(T_{Bn})K_n$ by creating an authentication table composed of precalculated encrypted code elements for the identification media for the temporal sequence of values (T_{Bn}), and further attempting to match encrypted code elements $(T_{Bn})K_n$ to the precalculated encrypted code elements in the authentication table.

22. The tracking method according to claim 21, wherein authenticating the encrypted code elements includes encrypting a temporal sequence of values (T_{Bn}) and an offset time value (T_{on}) for each identification medium with a corresponding

unique private key K_n to generate a list of encrypted code elements, En, as represented by the following expression:

$$En = (T_{Bn} + T_{on})_{Kn}.$$

23. A wireless identification system for use with an identification medium to provide access to a resource, comprising:

a sequence generator to generate a temporal sequence of values (TBn);

a private key Kn unique to the identification medium;

an encryptor to receive a temporal sequence value and the private key, and to output an encrypted result;

a transmitter module secured to the identification medium to receive the encrypted result and to output a wireless signal;

a receiver module to receive the wireless signal and output the encrypted result; and

an authenticator, to receive the encrypted result and the private key Kn, and to output an access authorization signal.

24. The wireless identification system according to claim 23, for use with a plurality of identification media, each identification medium including a transmitter module and a unique private key for transmitting one or more of the encrypted results to the receiver module for authentication.

25. The wireless identification system according to claim 24, wherein the authenticator stores private keys of the plurality of identification media.

26. The wireless identification system according to claim 23, wherein the authenticator pre-calculates future encrypted results.

27. The wireless identification system according to claim 26 wherein the future encrypted results are distributed to a remote authenticator to enable time-limited access to a resource.

28. The wireless identification system according to claim 24, wherein the temporal sequence of values is measured from an initial synchronized starting point of each identification medium.

29. The wireless identification system according to claim 24, wherein the temporal sequence of values is incremented in equal time increments.

30. The wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal periodically.

31. The wireless identification system according to claim 24, wherein the transmitter module outputs the wireless signal upon external stimulus, wherein the external stimulus is any one or more of: a mechanical switch, a motion detector, a light detector, or a sound detector.

32. The wireless identification system according to claim 24, wherein the authenticator creates an authentication table composed of pre-calculated encrypted code elements for every identification medium, and further attempts to match the

encrypted code elements transmitted by the transmitter module to the pre-calculated encrypted code elements in the authentication table.

33. The wireless identification system according to claim 24,wherein the temporal sequence of values (TBn) is represented by the following expression;

$$(TBn)=Tsystem-Tn\ creation,$$

where Tsystem represents current time for the authenticator, and Tn creation represents a creation time of the identification medium referenced to a same time standard as Tsystem; and

wherein the server stores Tn creation for each identification medium.

34. The wireless identification system according to claim 33, wherein the authenticator establishes a clock synchronization window for the list of authentication codes, En, to account for time drift between the current time of the identification medium and a current time of the authenticator.

35. The wireless identification system according to claim 34, wherein the clock synchronization window is centered around the current time (TBn) of the identification medium, as shown by the following expressions:

$$En1 = (TBn + Ton)Kn,$$

$$En2 = (TBn + Ton - Epsilon)Kn, \text{ and}$$

$$En3 = (TBn + Ton + Epsilon)Kn,$$

where En1 is an authentication code when the identification medium is in general synchrony with the server;

where En2 is an authentication code when the identification medium lags the server;

where En3 is an authentication code when the identification medium leads the server; and

where Epilson is an resolution of the temporal sequence of values (TBn).

36. The wireless identification system according to claim 24, wherein the transmitter module is incorporated in any one or more of: an identification badge, a card, or a label.

37. The wireless identification system according to claim 36, wherein the identification medium includes any one or more of: a credit card, a dining card; a telephone calling card; a health card; a driver's license; a video store card; a car access card; a computer access card; or a building access card; an identification tag, a key fob.

38. The wireless identification system according to claim 25, wherein upon authenticating the identification medium, the authenticator provides authentication information to an application for initiating the application.

39. The wireless identification system according to claim 24, wherein the authenticator encrypts the temporal sequence of values (TBn) and an offset time value (Ton) for each identification medium with a corresponding unique private key Kn to generate a list of authentication codes, En, as represented by the following expression:

$$En = (TBn + Ton)Kn.$$

SYSTEM AND METHOD FOR PROVIDING TIME-LIMITED ACCESS TO PEOPLE, OBJECTS AND SERVICES

ABSTRACT OF THE INVENTION

A limited tracking system and associated method that enable the use of personal encoded identification media to limit access to tracking information. The tracking system provides concurrent time-limited access to a large number of people, objects, information, services, and other resources, and has particular applicability to credit cards, dining cards, telephone calling cards, health cards, driver's licenses, video store cards, car access cards, building access cards, computer access cards, and like identification badges or cards. The tracking system includes a transmitter module incorporated in a badge, and a receiver module incorporated in a secure server. The transmitter module contains an encryptor and a watch crystal that keeps track of time, such that the encryptor encrypts the current time with the user's private key, and periodically transmits the encrypted current time to the receiver module, as a code list. The server stores the private keys of all the users, and, in turn, encrypts the current times of all the badges with the corresponding private keys of the users, to generate an authentication table. An authenticator compares the received code list to the authentication table, seeking matches that are indicative of the validity of the transmitting badges.

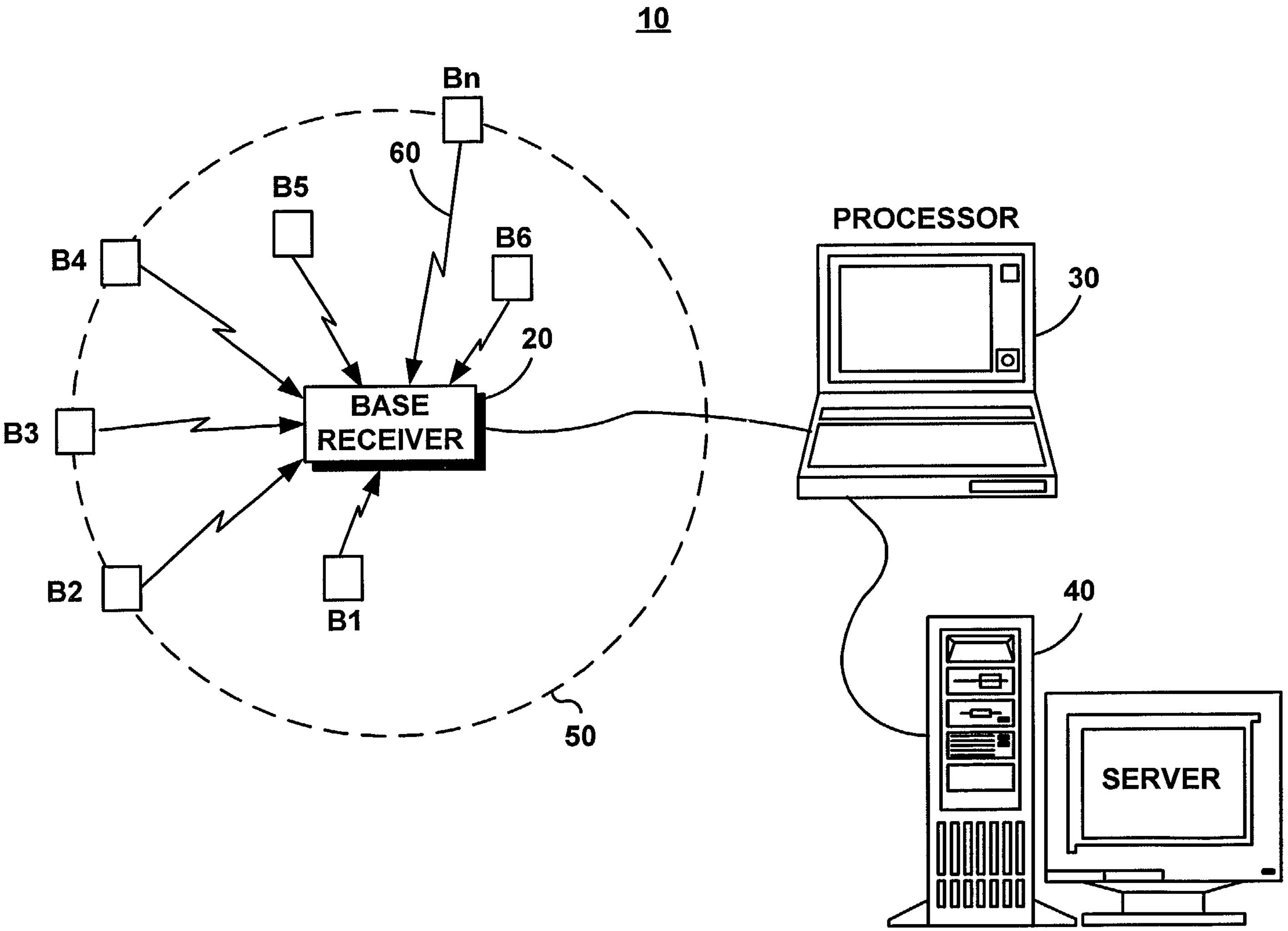
10
Bn
60
B5
B6
B4
20
BASE RECEIVER
B3
B2
B1
50
PROCESSOR
30
40
SERVER

FIG. 1

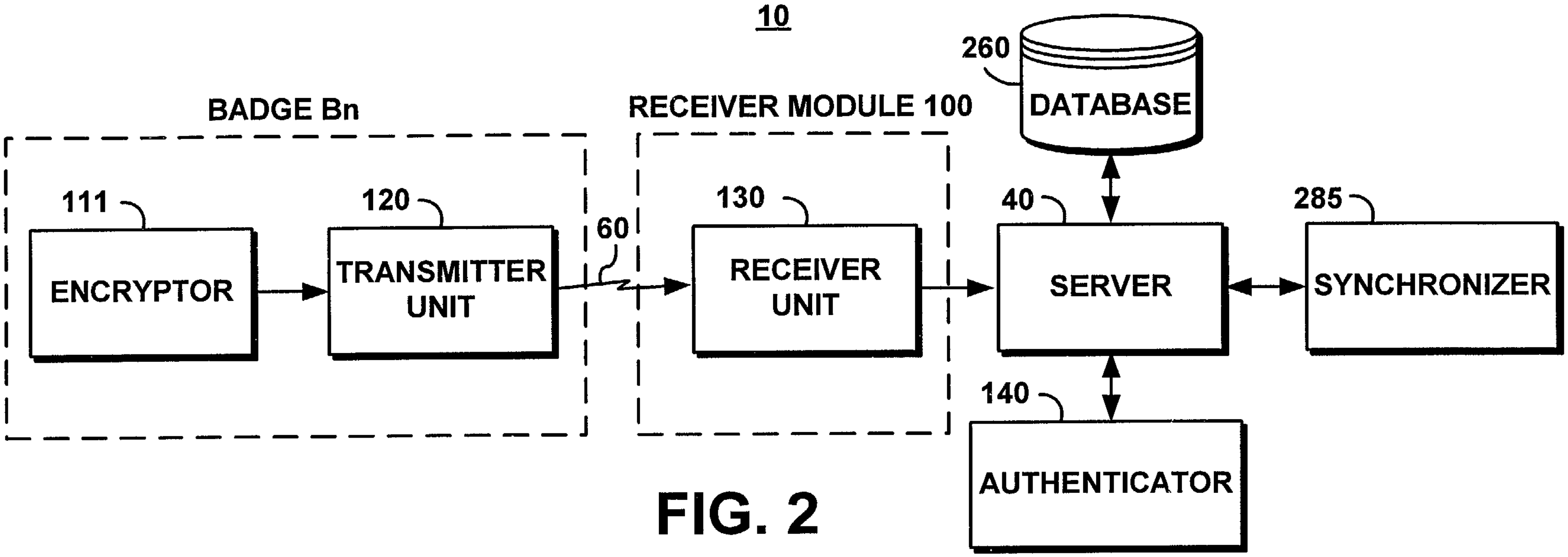
10
BADGE Bn
111
ENCRYPTOR
120
TRANSMITTER UNIT
60
RECEIVER MODULE 100
130
RECEIVER UNIT
260
DATABASE
40
SERVER
285
SYNCHRONIZER
140
AUTHENTICATOR

FIG. 2

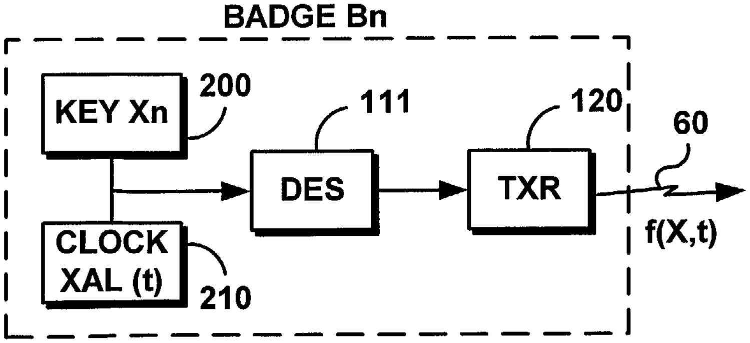
BADGE Bn
KEY Xn
200
CLOCK XAL (t)
210
111
DES
120
TXR
60
f(X,t)

FIG. 3

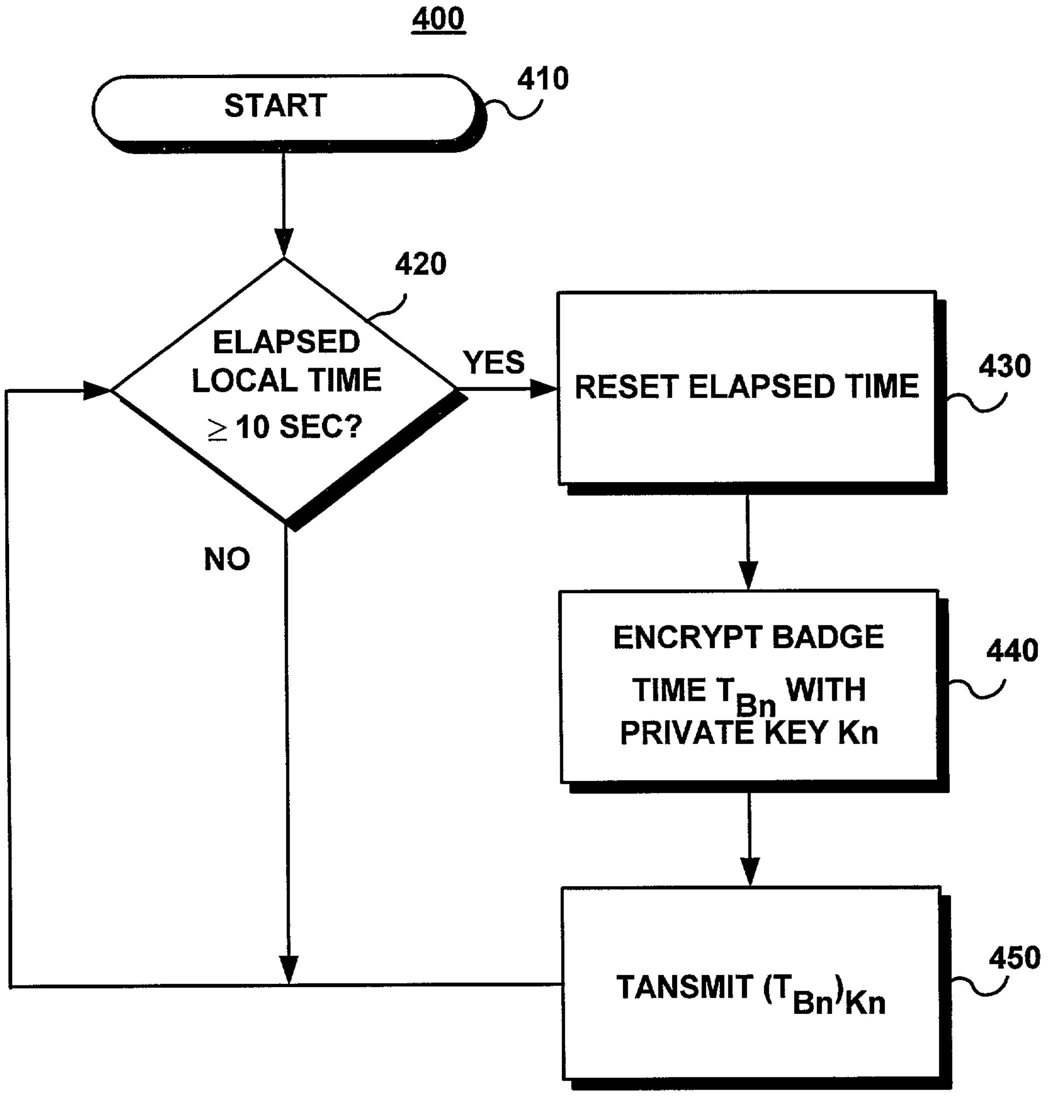
400
START
410
420
ELAPSED LOCAL TIME ≥ 10 SEC?
YES
NO
RESET ELAPSED TIME
430
ENCRYPT BADGE TIME T_{Bn} WITH PRIVATE KEY Kn
440
TANSMIT $(T_{Bn})_{Kn}$
450

FIG. 4

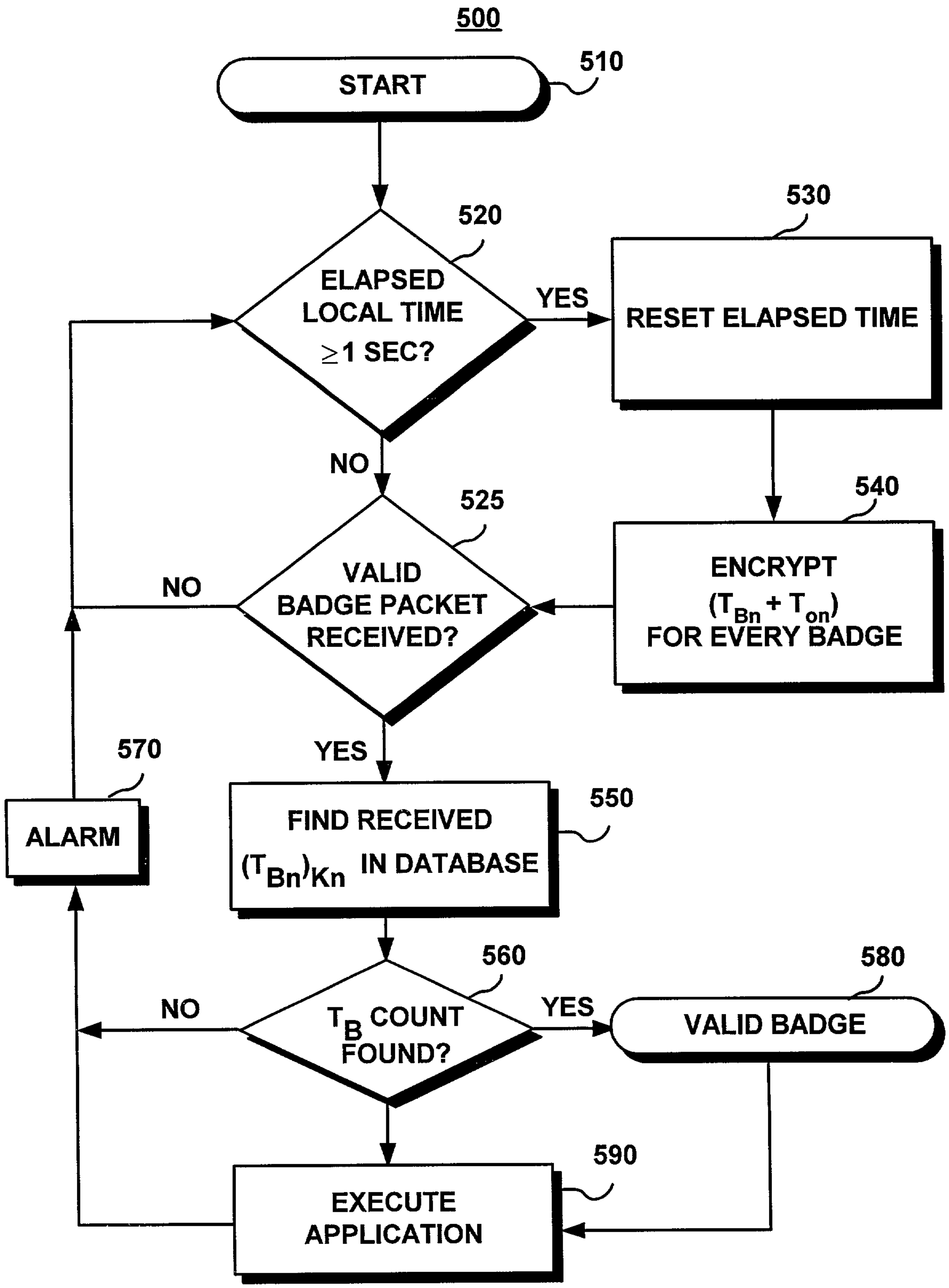
500
START
510
ELAPSED LOCAL TIME ≥1 SEC?
520
YES
RESET ELAPSED TIME
530
NO
VALID BADGE PACKET RECEIVED?
525
NO
ENCRYPT (T_{Bn} + T_{on}) FOR EVERY BADGE
540
YES
FIND RECEIVED (T_{Bn})$_{Kn}$ IN DATABASE
550
ALARM
570
T_B COUNT FOUND?
560
NO
YES
VALID BADGE
580
EXECUTE APPLICATION
590

FIG. 5

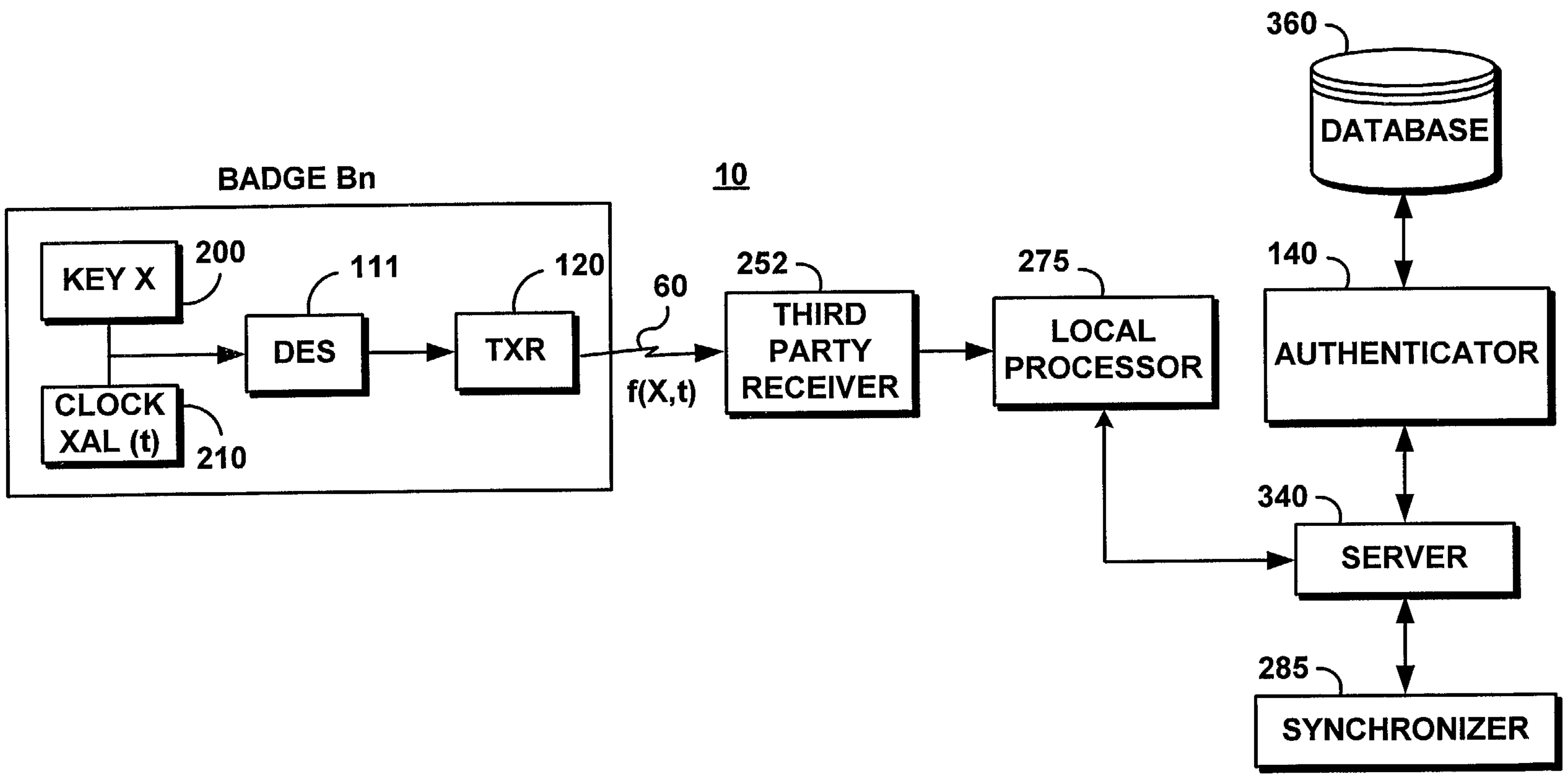
BADGE Bn
10
KEY X
200
DES
111
TXR
120
CLOCK XAL (t)
210
60
f(X,t)
252
THIRD PARTY RECEIVER
275
LOCAL PROCESSOR
360
DATABASE
140
AUTHENTICATOR
340
SERVER
285
SYNCHRONIZER

FIG. 6

Page 1 of 2 Docket No. ARC9–2000-0091-US1

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

//

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

"SYSTEM AND METHOD FOR PROVIDING TIME-LIMITED ACCESS TO PEOPLE, OBJECTS AND SERVICES"

the specification of which is attached hereto unless the following box is checked:
was filed on ____________________
as United States Application Number or PCT International Application Number ____________________
and was amended on ____________________ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 USC §119(a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s): Priority Not Claimed

__________ __________ __________ X
(Number) (Country) (Day/Month/Year Filed)

I hereby claim the benefit under 35 USC §119(e) of any United States provisional application(s) listed below:

Provisional Application(s): __________ __________
(Application Number) (Filing Date)

I hereby claim the benefit under 35 USC §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 USC §112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

__________ __________ __________
(Application Number) (Filing Date) (Status - patented, pending, abandoned)

Power of Attorney:

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Richard M. Ludwin	(#33,010)	Marc D. McSwain	(#44,929)
Thomas R. Berthold	(#28,689)	Alison D. Mortginger	(#39,306)
Khanh Q. Tran	(#41,352)	Samuel A. Kassatly	(#32,247)

Page 2 of 2 Docket No. ARC9–2000-0091-US1

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

//

Address all telephone calls to:
Samuel A. Kassatly

(408) 323-5111

Address all correspondence to:
Samuel A. Kassatly
6819 Trinidad Drive
San Jose, California 95120

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

//

Full name of sole or first inventor: **ZIMMERMAN**, Thomas Guthrie

Inventor's signature: Thomas G. Zimmerman Date: 9/27/2000

Residence: 7611 Hollanderry Place
Cupertino, CA 95014

Citizenship: USA Post Office Address: Same

//

Full name of second inventor:

Inventor's signature: Date:

Residence:

Citizenship: Post Office Address:

//